

Fig. 1

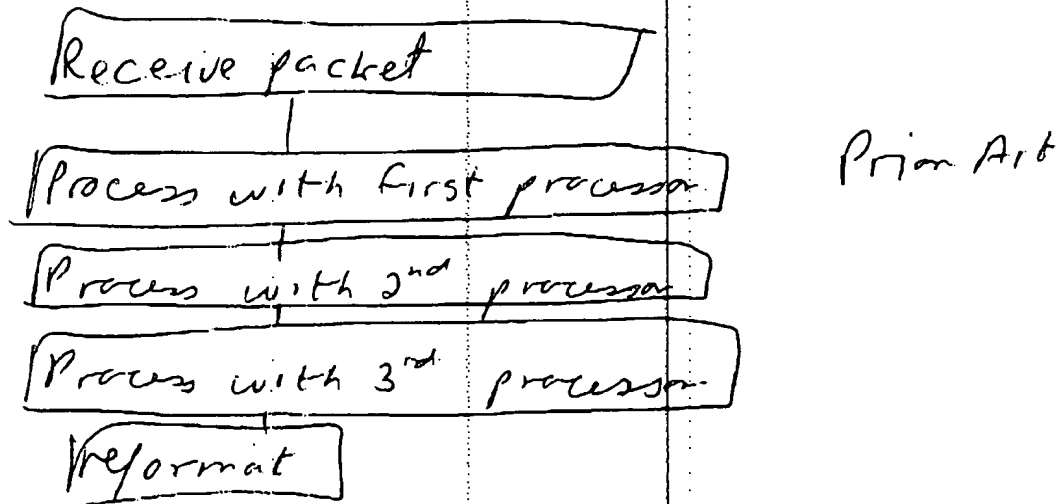


Fig. 2

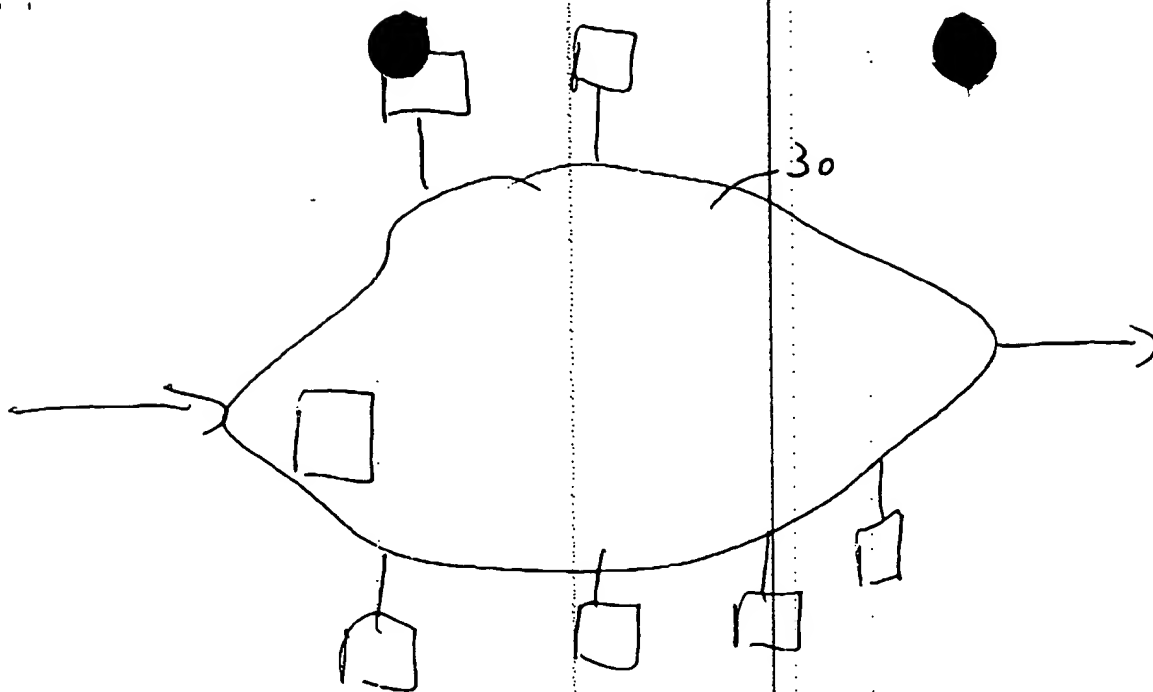


Fig. 3

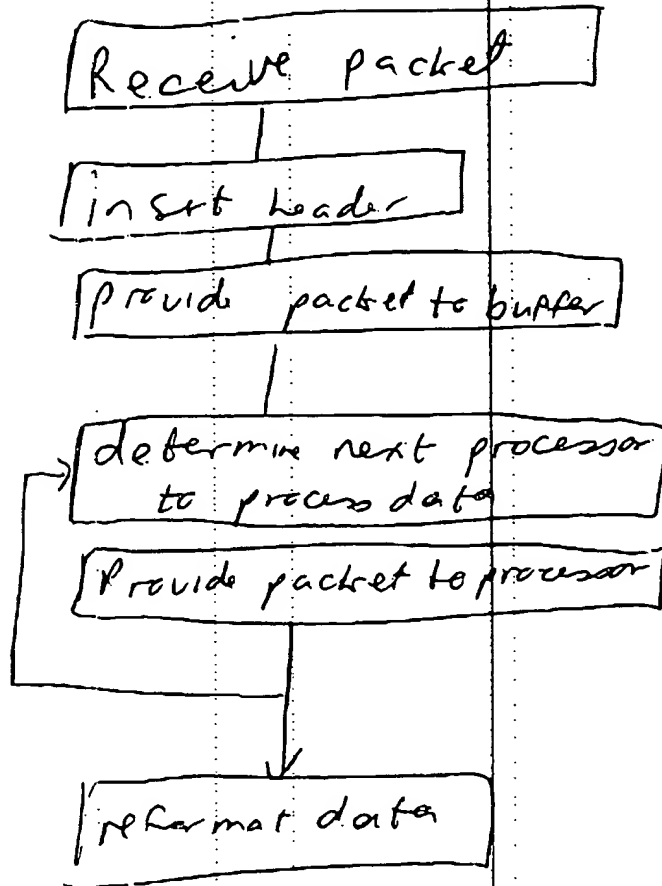
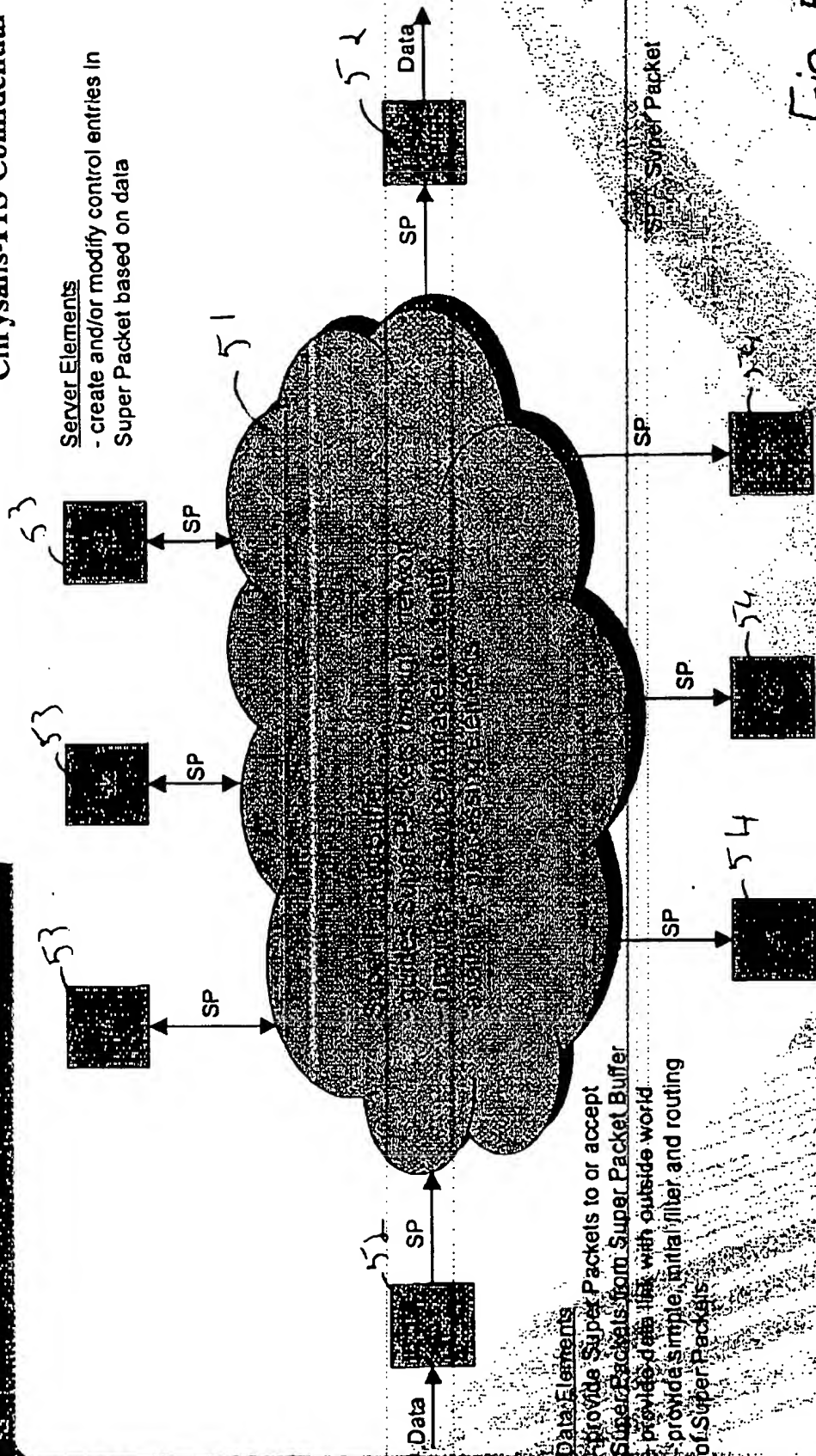


Fig. 4

Chrysalis-ITS Confidential

Server Elements

- create and/or modify control entries in Super Packet based on data

Data Elements

- provide Super Packets to or accept Super Packets from Super Packet Buffer
- provide data link with outside world
- provide simple, initial filter and routing of Super Packets

Client Elements

- perform simple processing functions on data as specified in Super Packet control entries
- can modify data and associated control entries in the Super Packet
- can not add or subtract control entries in Super Packet

Generic Processing Element

- can interact with a super packet and super packet buffer
- can modify control and data elements of super packet

Fig. 5

27 November 2000

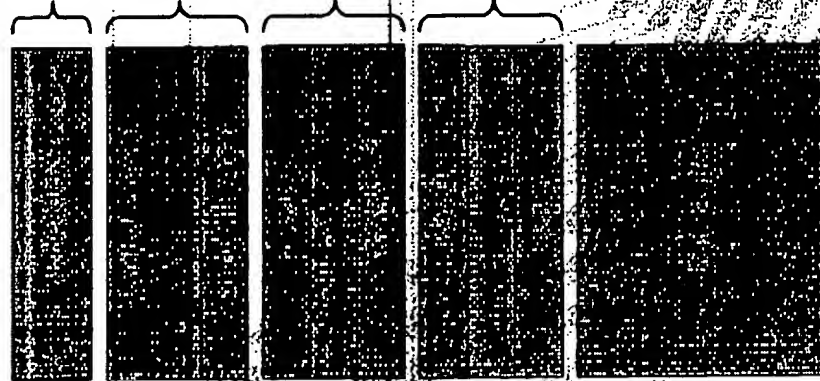
Copyright 1999-2000 Chrysalis-ITS, Inc. All rights reserved.

Chrysalis-ITS

Chrysalis-ITS Confidential

Super Packet

- Contains all control, coding, keying information required to process the contained data



Header identifies Super Packet and provides timing and tracking information.

Control Entries identify operation to be performed on attached data and how to treat result data. result codes and completion information are placed back into the control entries.

uCode is the instructions required by the generic control elements to perform the commands coded in the control entries on the associated data.

Keying information must be provided for each control action that invokes a cryptographic operation.

Data buffer controls original and modified data.

Fig 6

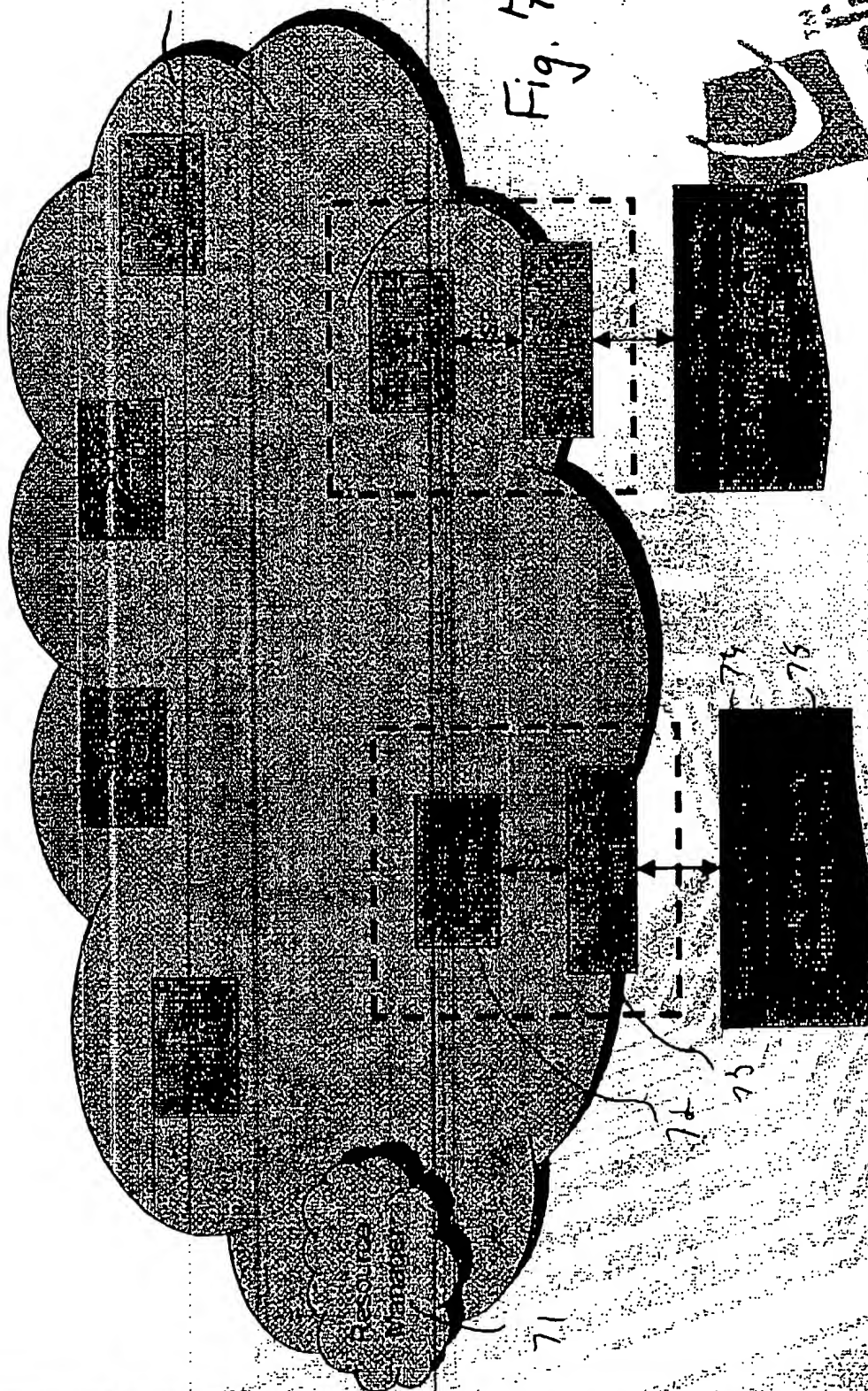


27 November 2000

Copyright 1999-2000 Chrysalis-ITS, Inc. All rights reserved.

Super Packet Buffer

- Responsible for moving Super Packet between the generic processing elements

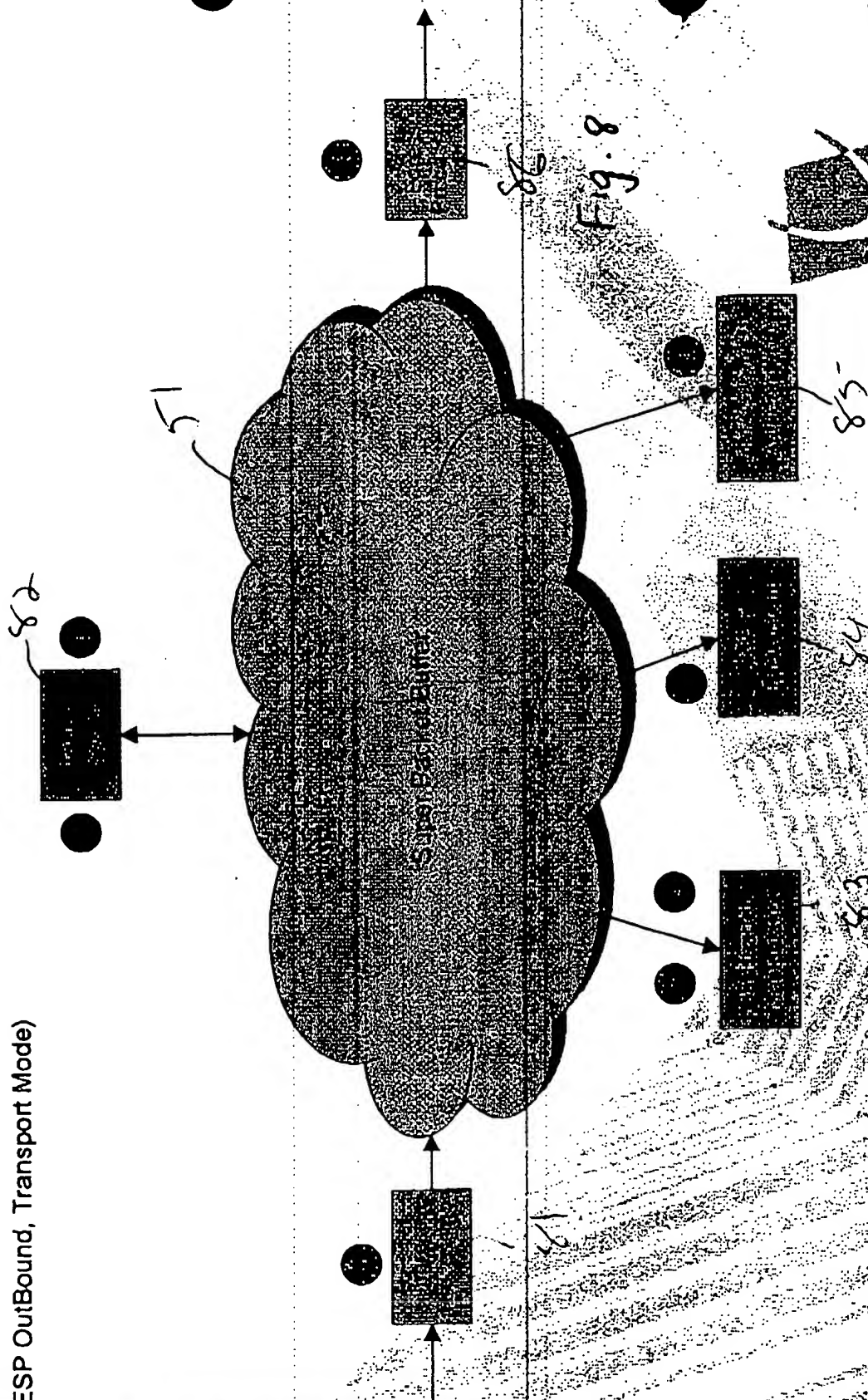


EMPOWERING NEXT GENERATION NETWORK SECURITY

Chrysalis-ITS Confidential

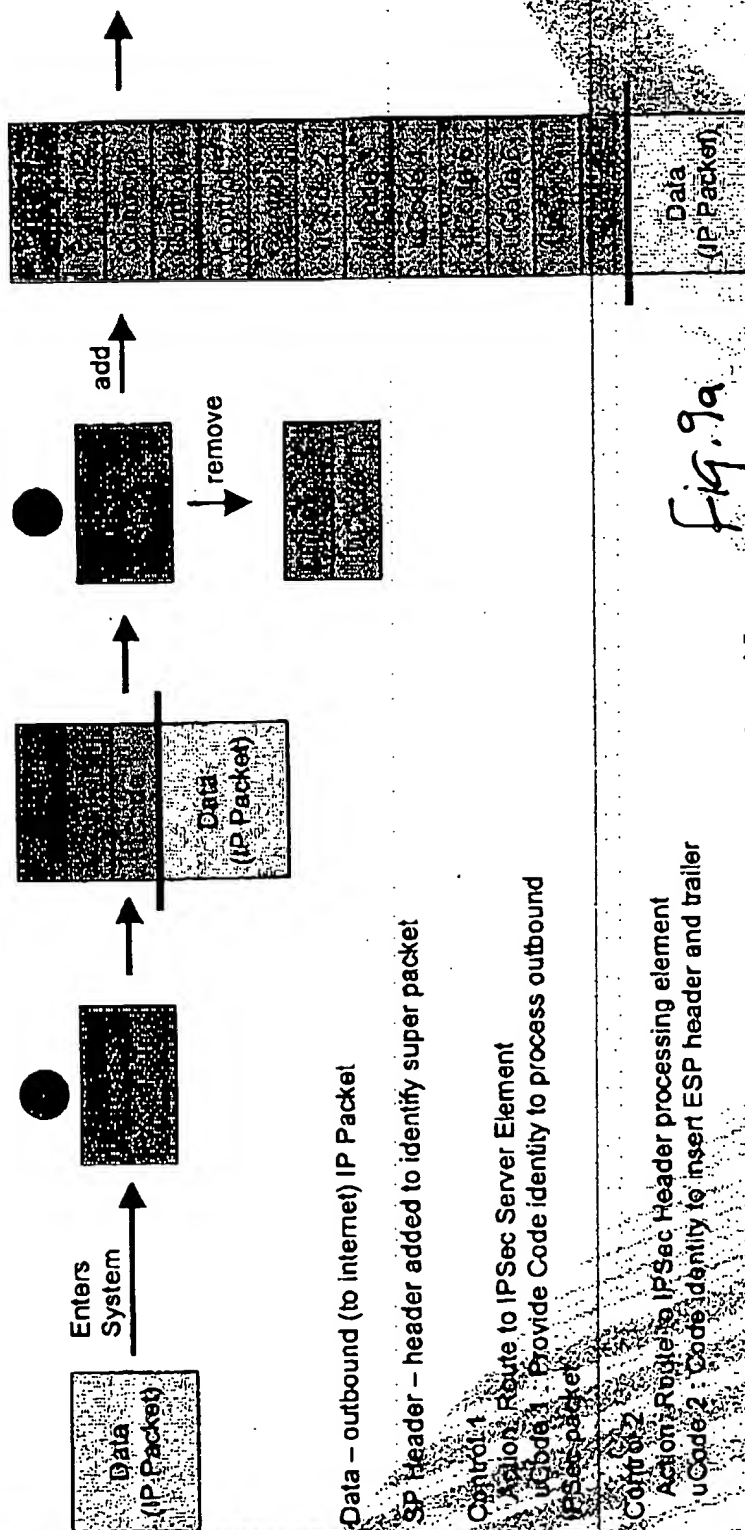
IPSec Processing Example

(ESP OutBound, Transport Mode)



Chrysalis-ITS Confidential

IPSec Super Packet (1)



Data - outbound (to Internet) IP Packet

SP Header - header added to identify super packet

Control 1

Action: Route to IPSec Server Element

uCode 1: Provide Code identity to process outbound

IPSec packet

Control 2

Action: Route to IPSec Header processing element

uCode 2: Code identity to insert ESP header and trailer

Control 3

Action: Route to 3DES processing element and encrypt

uCode 3: 3DES algorithm (CBC Mode)

Key 3: 3DES key for packet

Control 4

Action: Route to HMAC96-MD5 processing element and

generate MAC

uCode 4: HMAC96-MD5 algorithm

Key 4: HMAC Key for packet

Fig. 9a

Control 5

Action: Place MAC in ESP Header

uCode 5: Code identity for post encryption header

manipulation

Control 6

Action: Route to Egress Unit

uCode 6: Code identity to strip new IP Packet from

Packet and transmit

27 November 2000

Copyright 1999-2000 Chrysalis-ITS, Inc. All rights reserved.

Chrysalis-ITS

The diagram illustrates the construction of an IPsec packet through several stages of encryption and encapsulation. It is divided into three main horizontal sections, each representing a different stage of the process, with arrows indicating the flow from left to right.

- Top Section:** Shows the initial state where a single **IP Packet** is encapsulated. The resulting structure consists of four main components: **IP Header**, **ESP Header**, **IP Packet**, and **ESP Trailer**. This structure is then encrypted by **Code 1** and **Code 2** to produce a **Code 1** block and a **Code 2** block. These are then combined into a single **Code 1** block and a **Code 2** block, which are then combined into a single **Code 1** block and a **Code 2** block. Finally, the entire structure is encrypted by **Code 3** to produce the final **IP Header**, **ESP Header**, **ESP Trailer**, **IP Packet**, and **ESP Trailer** structure.
- Middle Section:** Shows the intermediate state where the **IP Packet** is encapsulated with **ESP Header** and **ESP Trailer**. This structure is then encrypted by **Code 1** and **Code 2** to produce a **Code 1** block and a **Code 2** block. These are then combined into a single **Code 1** block and a **Code 2** block, which are then combined into a single **Code 1** block and a **Code 2** block. Finally, the entire structure is encrypted by **Code 3** to produce the final **IP Header**, **ESP Header**, **ESP Trailer**, **IP Packet**, and **ESP Trailer** structure.
- Bottom Section:** Shows the final state where the **IP Packet** is encapsulated with **ESP Header** and **ESP Trailer**. This structure is then encrypted by **Code 1** and **Code 2** to produce a **Code 1** block and a **Code 2** block. These are then combined into a single **Code 1** block and a **Code 2** block, which are then combined into a single **Code 1** block and a **Code 2** block. Finally, the entire structure is encrypted by **Code 3** to produce the final **IP Header**, **ESP Header**, **ESP Trailer**, **IP Packet**, and **ESP Trailer** structure.

96.514

Cross hatch indicates processing complete.

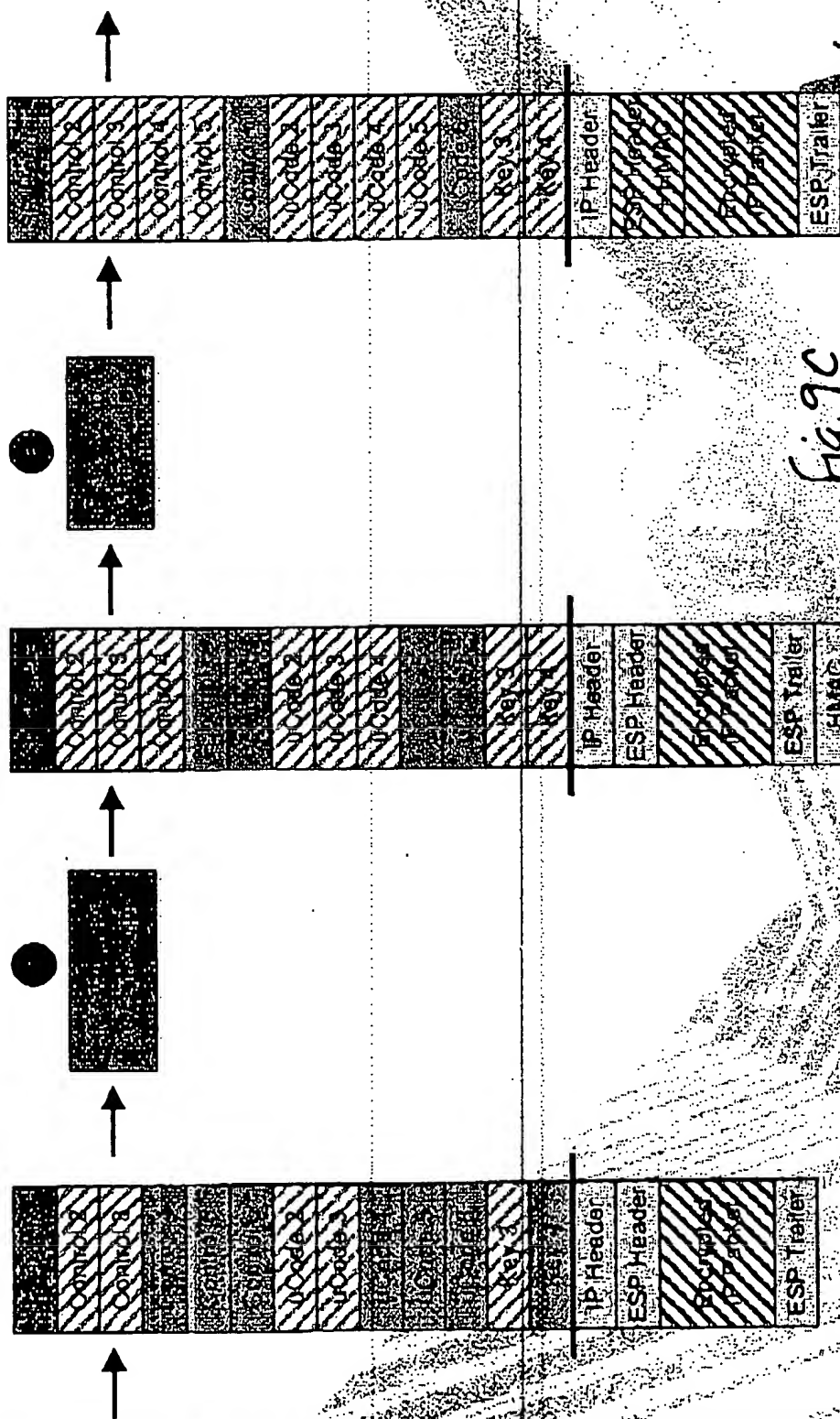
Copyright 1998-2000, Chrysalis-TS, Inc. All rights reserved.

27 November 2000



Chrysalis-ITS Confidential

IPSec Super Packet (3)



Cross hatch indicates processing complete

Copyright 1999-2000, Chrysalis-ITS, Inc. All rights reserved.

27 November 2000

Chrysalis-ITS

EMPOWERING NEXT GENERATION NETWORK SECURITY

Chrysalis-ITS Confidential

IPSec Super Packet (4)

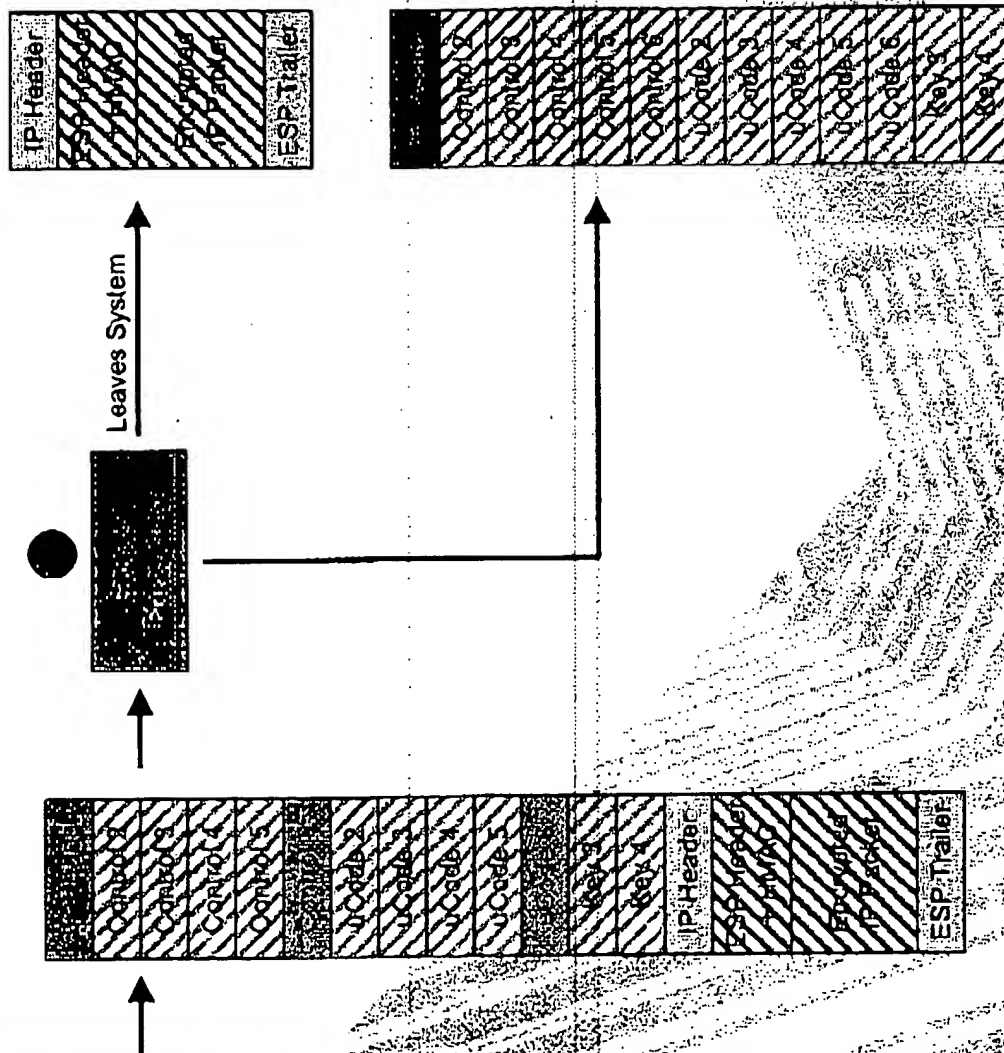


Fig. 9d



27 November 2000

Copyright 1998-2000, Chrysalis-ITS, Inc. All rights reserved.

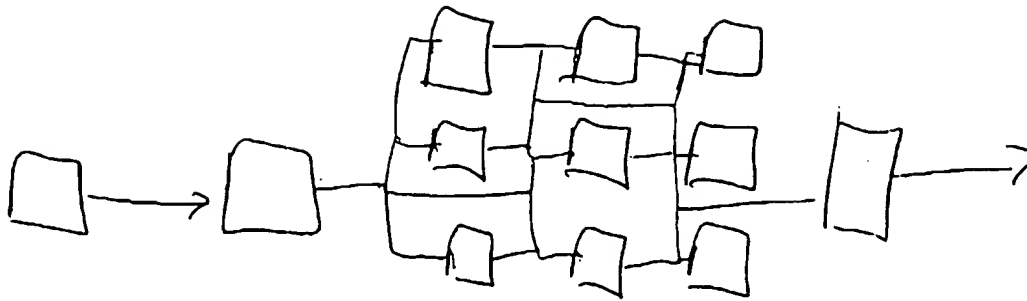


Fig-10